Host-based DoS Attacks and Defense in the Cloud

Tianwei Zhang and Ruby B. Lee
Princeton University

HASP
June 25, 2017

Denial-of-Service in the Cloud

- □ Denial-of-Service attacks
  - Compromise the **availability** of system and services.
  - Network-based (Distributed) DoS attacks.
- □ Cloud becomes an important target
  - Top threats in cloud computing[1].
  - 86% of service providers witnessed DDoS attacks[2] in 2016.
- □ Host-based DoS attacks
  - Shared computing resources (memory, I/O devices)

[1] Top Threats Working Group. The Treacherous 12 Cloud Computing Top Threats in 2016. In Cloud Security Alliance, 2016

[2] Arbor Networks, Worldwide Infrastructure Security Report, 2016

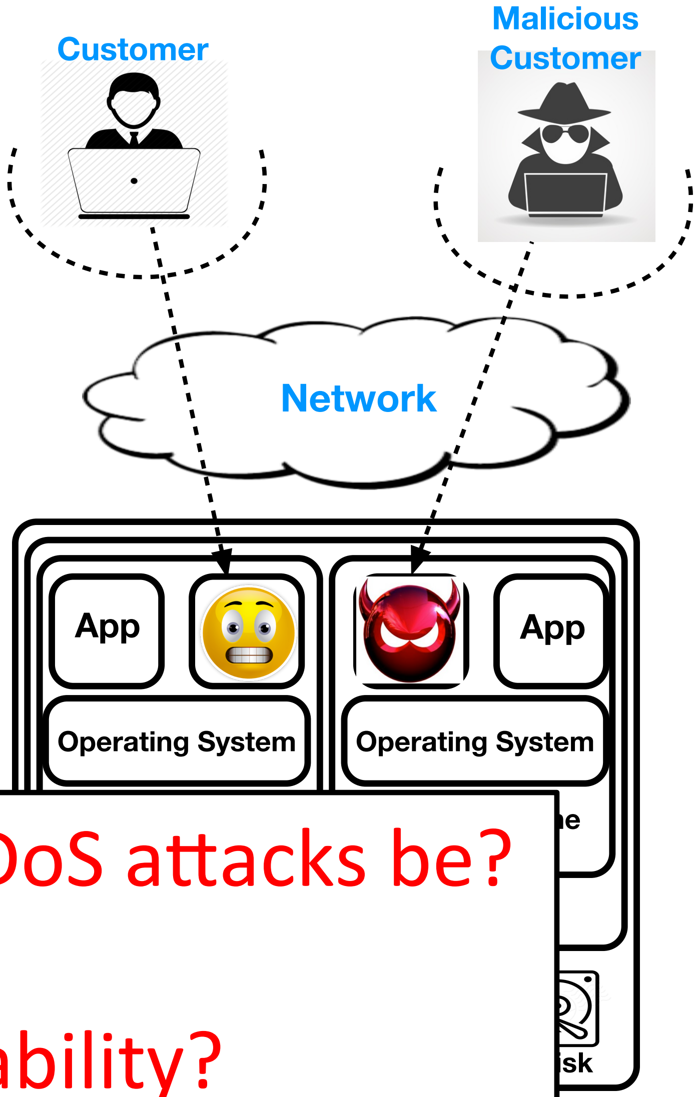
Multi-tenancy Vulnerability

□ Infrastructure-as-a Service

- Customers lease Virtual Machines

□ Multi-tenancy

□ New Vulnerability



How severe can host-based DoS attacks be?

How to mitigate such vulnerability?

Outline

- Host-based DoS attacks.
  - Attack techniques.
  - Server-wide attacks
  - Datacenter-wide attacks
- Defense.
  - Monitoring
  - Identifying attacker VMs

Threat Model and Assumptions

❑ Attacker's Goal.

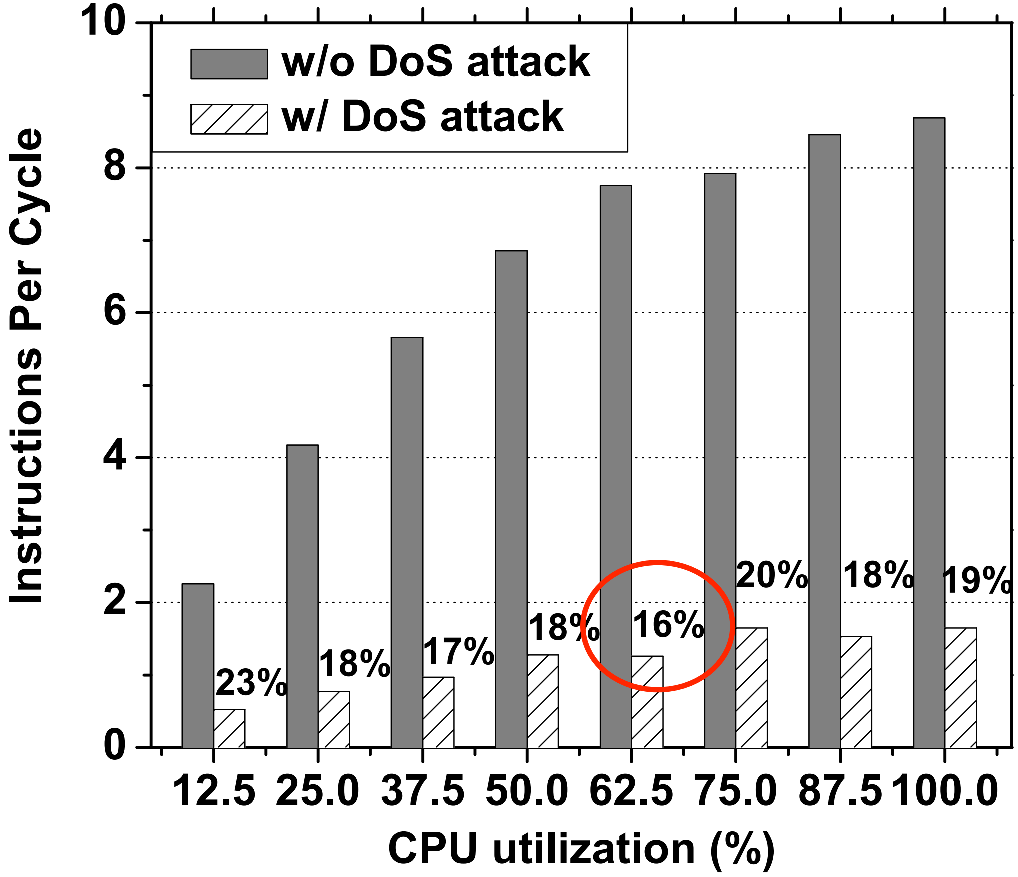
- Compromise the availability of cloud servers and the datacenter

❑ Attacker's capability.

- Can launch multiple VMs in the target datacenter
- Has full control of his own VMs, but not the hypervisor or other VMs.

Memory DoS Attack

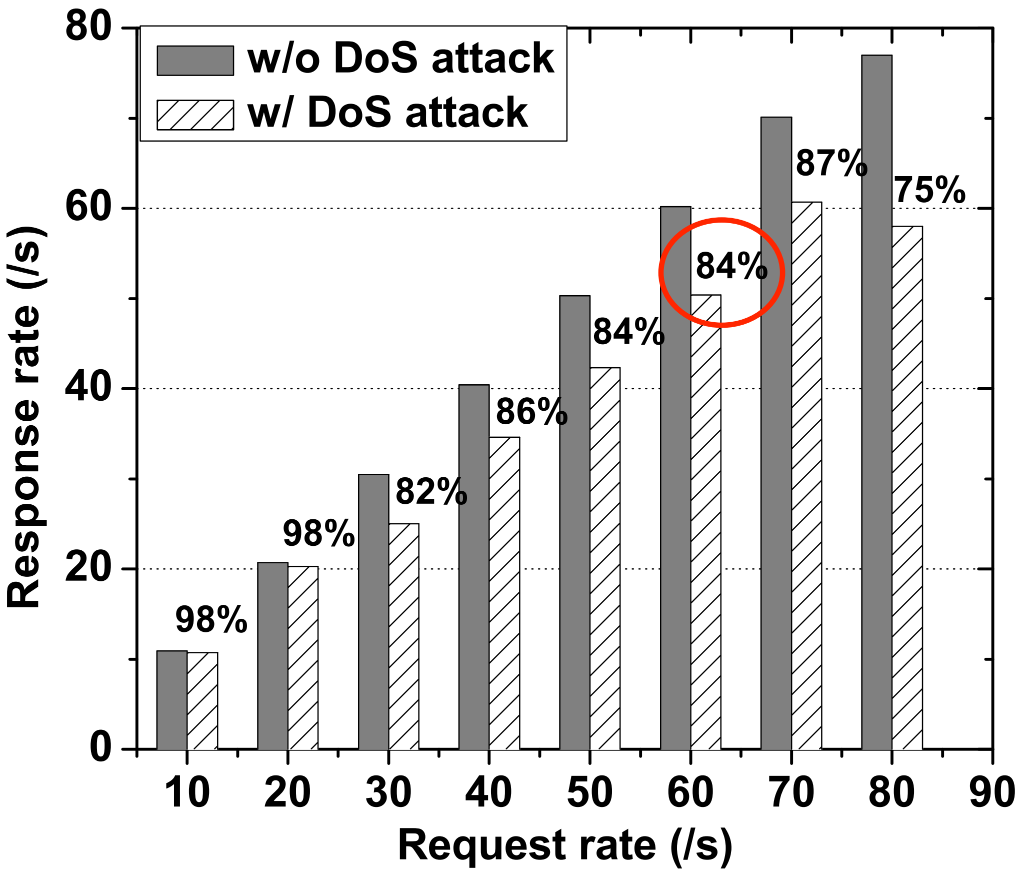
- Memory Contention
  - Exotic locked atomic operation (atomic access to unaligned blocks) can lock the memory bus.



Network DoS attacks

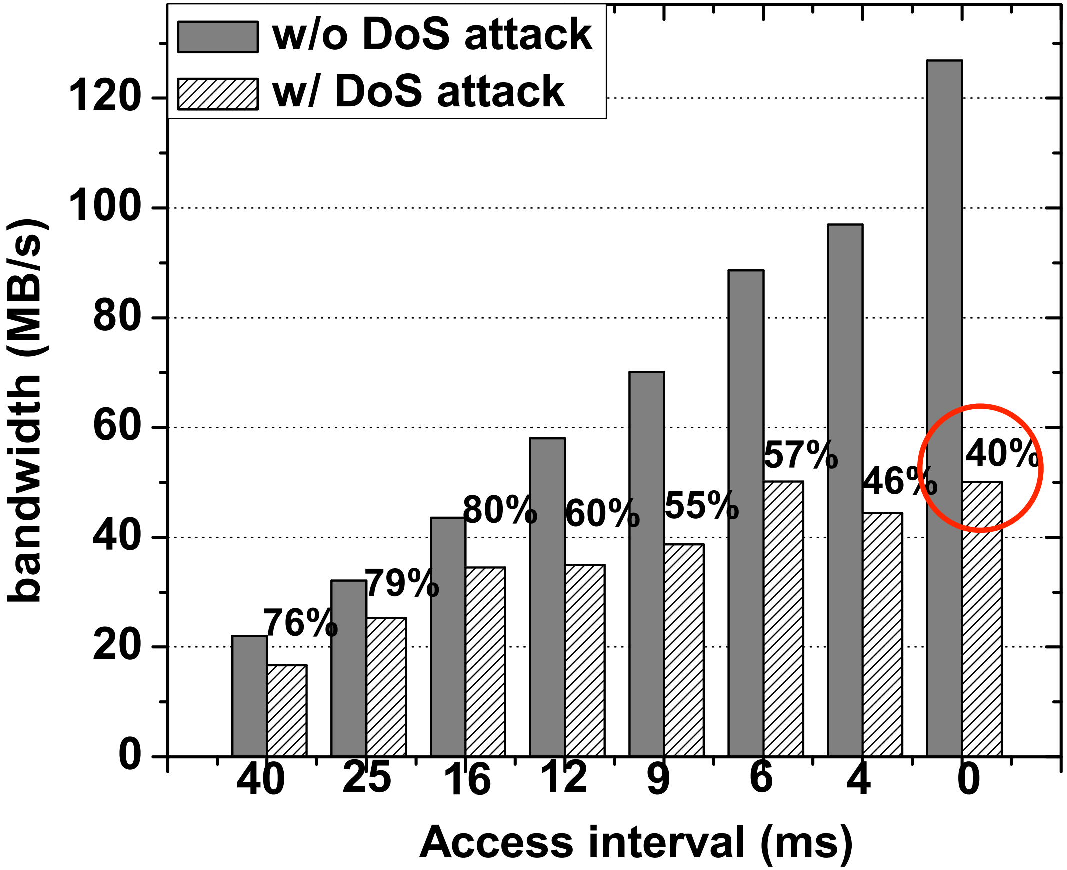
❑ Network DoS attacks.

- Flood the VM with network packets to cause congestion in the physical devices and deplete the hypervisor's ability to handle network inputs and outputs for VMs



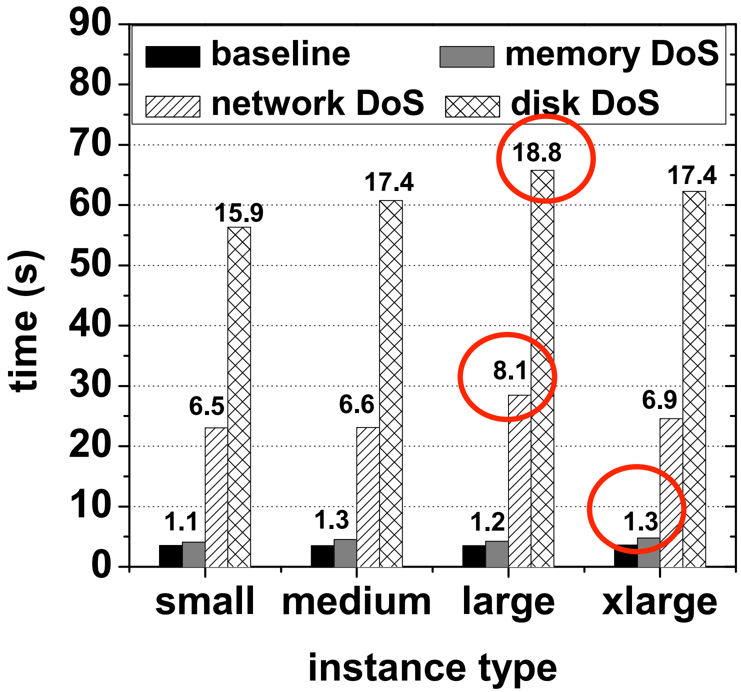
Disk DoS attacks

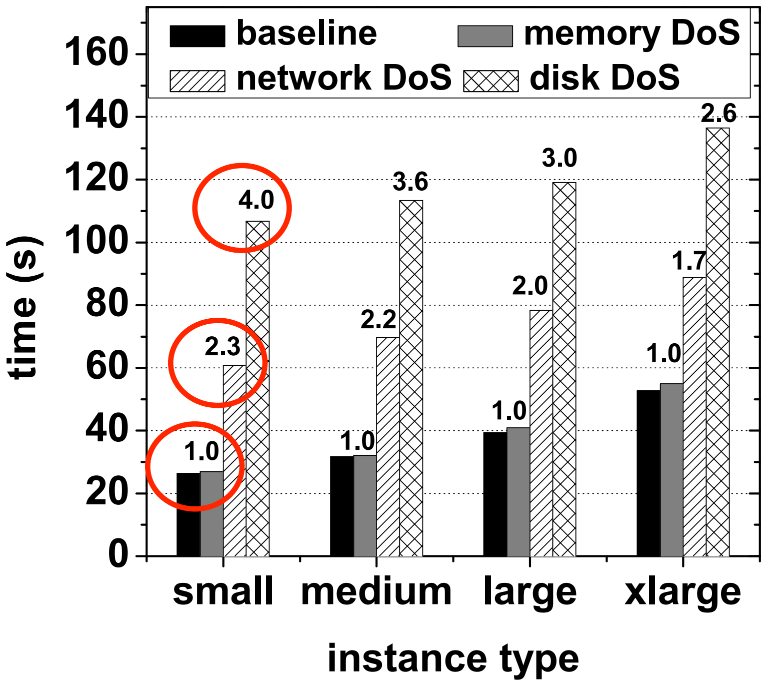
- Disk DoS attacks.
  - Flood the VM with disk accesses to cause congestion in disk scheduler and devices



Evaluation: Attacking Cloud Providers

- ❑ Affecting cloud provider's management services
  - OpenStack
- ❑ VM launch
  - Memory: 1.3X; Network: 8.1X; Disk: 18.8X
- ❑ VM migration.
  - Memory: 1.0X; Network: 2.3X; Disk: 4.0X



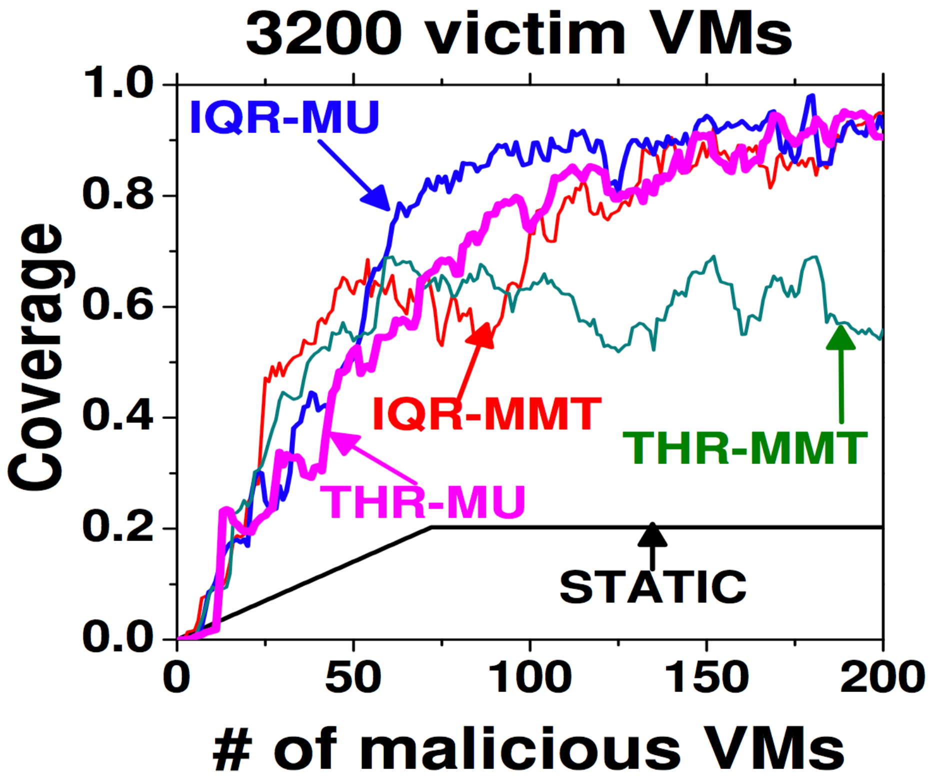


Attacking the Entire Datacenter

- ❑ Attacker launches a large number of VMs to cover as many servers as possible
- ❑ Power-aware VM scheduling policies make this easier for attacker
  - VM launch: allocate VMs on the smallest number of servers (**STATIC**)
  - VM runtime: checks if each server is overloaded:
    - Static threshold (**THR**)
    - Interquartile Range (**IQR**)
  - Select some VMs and migrate them to other servers
    - Minimum Migration Time (**MMT**)
    - Minimum Utilization (**MU**)

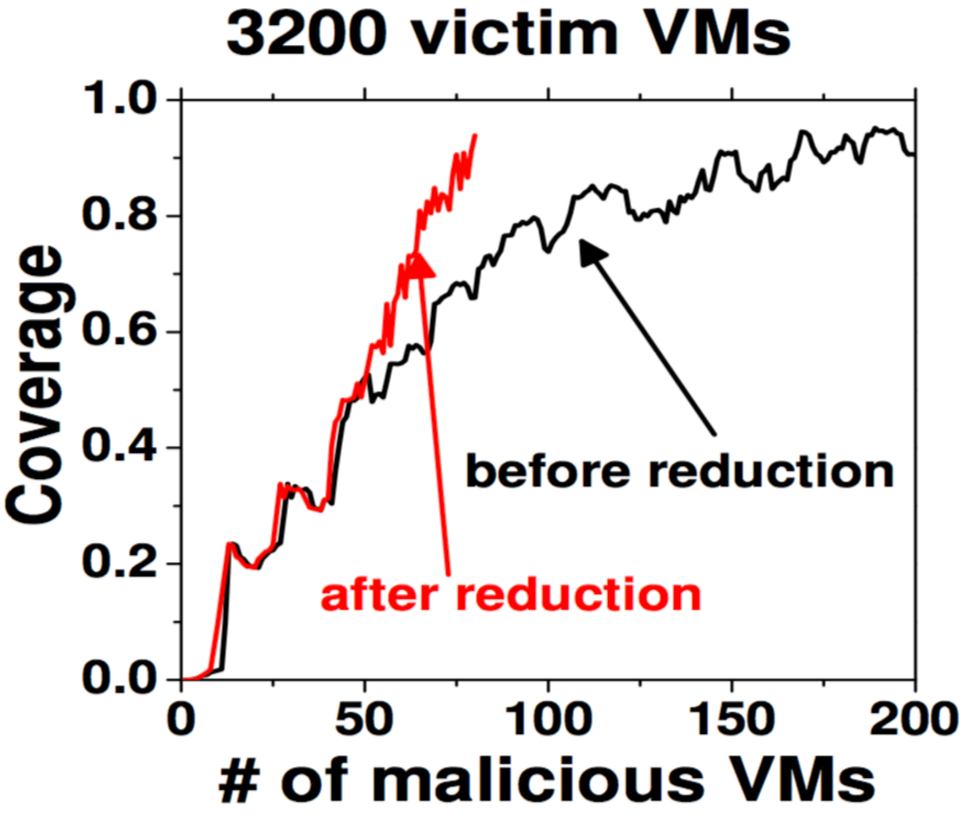
Evaluating Datacenter-wide Attacks

- ❑ Use CloudSim to simulate a cloud system
- ❑ Attacker's coverage
  - # of infected servers / # of active servers
- ❑ Power-aware policies are more vulnerable to attacks



Making Attacks More Efficient

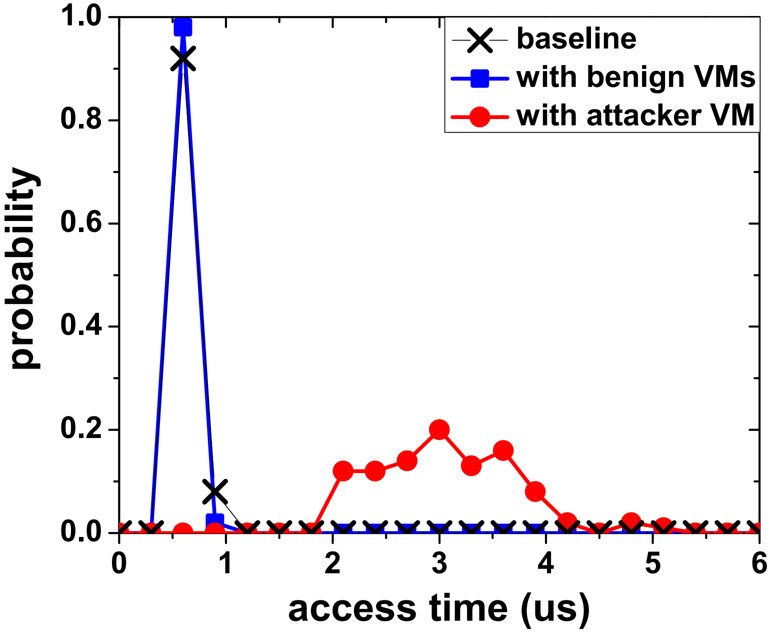
- ❑ Reducing co-located VMs
- ❑ Identify co-located VMs
  - Micro-architectural covert-channel technique
- ❑ Keep one VM on each server



A General-purpose Defense Solution

- ❑ Challenges.
  - Can detect different types of DoS attacks

- ❑ Key insights
  - A program's access characteristics to one computing resource follow a certain probability distribution
  - A huge change in a program's resource usage indicates excessive resource contention, i.e., host-based DoS attacks



Monitoring

❑ Run a Testing Program for each resource

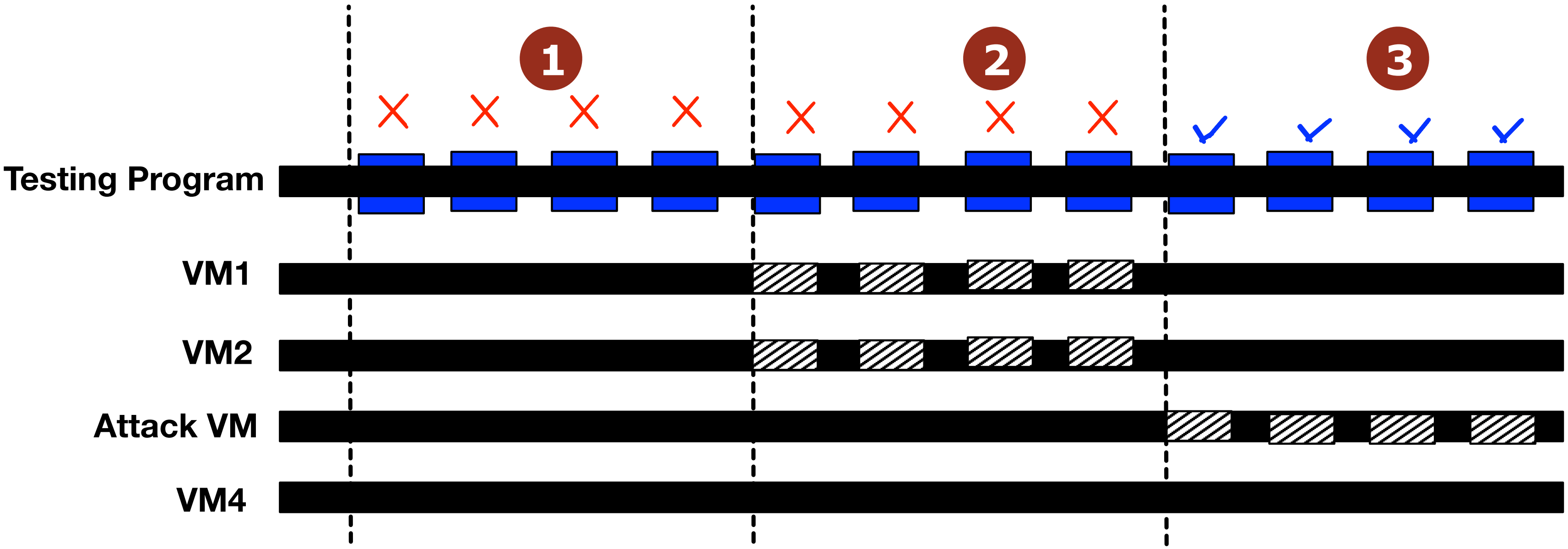
- Memory:
  - Access a fixed size of memory buffer.
  - Measure access time as a sample
- Network:
  - Establish a TCP connection.
  - Measure connection time as a sample
- Disk:
  - Access a fixed size of disk file.
  - Measure access time as a sample.

❑ Kolmogorov-Smirnov (KS) test:

- Offline reference samples: $[X_1^{\mathrm{R}}, X_2^{\mathrm{R}}, \ldots, X_{n^{\mathrm{R}}}^{\mathrm{R}}]$
- Online monitored samples: $[X_1^{\mathrm{M}}, X_2^{\mathrm{M}}, \ldots, X_{n^{\mathrm{M}}}^{\mathrm{M}}]$
- KS-value: $D_{n^{\mathrm{M}},\, n^{\mathrm{R}}} = \sup_x \mid F_{n^{\mathrm{M}}}^{\mathrm{M}}(x) - F_{n^{\mathrm{R}}}^{\mathrm{R}}(x) \mid$

Identifying Attacker VMs

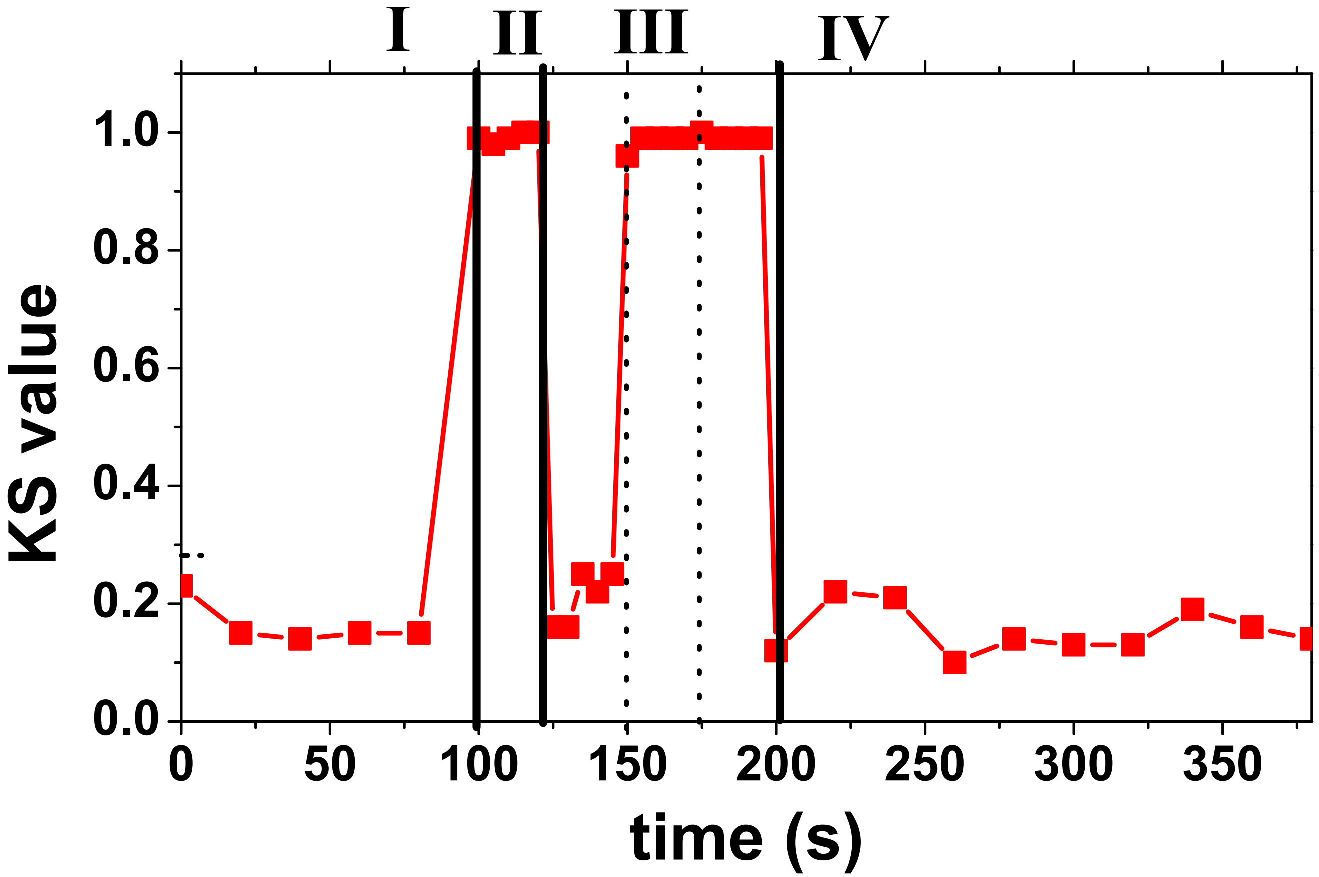
- Resource Throttling
  - Select parts of the VMs and throttle down their' execution.
  - Perform KS test to check if attacker VMs are within the selected VMs.
  - Using binary search to pinpoint the attacker VMs.
  - Throttling down or shut down the attacker VMs and notifying their owners.



Evaluation: Detection

❑ Four Stages

I. The attacker does nothing
II. The attacker begins attack
III. The cloud provider identifies the attacker VM
IV. The cloud provider shuts down the attacker VM



Conclusions

- ❑ Showing host-based DoS attacks on different resources that can cause availability degradation of entire cloud servers
- ❑ An attack strategy to compromise the availability of the entire datacenter
- ❑ Showing that power-aware scheduling policies make attacks on the whole data-center worse
- ❑ A novel general-purpose solution to defeat different DoS attacks using probability distribution sampling and resource throttling.

Thank You!